UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/580,438	05/24/2006	Ettore Elio Caprella	09952.0054	2553

22852 7590 09/08/2008

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/580,438	CAPRELLA ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see attachment*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the communications filed on 24 May 2006.

2. Claims 29-56 are pending in the application.

3. Claims 29-56 have been rejected.

4. Claims 1-28 have been cancelled.

Information Disclosure Statement

5. The examiner has considered the information disclosure statement (IDS) filed on 24 May 2006.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 29-37, 42-50, 55 and 56 are rejected under 35 U.S.C. 102(e) as being anticipated by Fox et al U.S. Patent No. 6,842,863 B1 (hereinafter Fox).

As to claim 29, Fox discloses a method of arranging communication between an administrator device and an administered device in a network, comprising the steps of:

> arranging the communication in the form of a chain of digitally signed communication items (i.e. the set of receipts/certificates generated by every transfer of the transaction forms a digitally-signed chain of evidence binding not only every step of the transaction but also every policy application that happened

along the way. Of course, it is feasible to include less information than the total accumulated with each additional transaction) [column 9, lines 52-67] including messages sent from an originator device to a recipient device, each the message having associated a respective digitally signed receipt (i.e. the relying party's policy is met, step 714 branches to step 718 where the reissue certificate 80 and relying party policy information are combined to form a receipt. The receipt is forwarded to the end entity 60 in step 720) [column 10, lines 43-47]; and

configuring the originator device not to send a new item toward the recipient device in the absence of a respective digitally signed receipt for a previously sent item [column 10, lines 48-58].

As to claims 30 and 43, Fox discloses the method, comprising the steps of:

detecting at the originator device a respective digitally signed receipt item from the recipient device having failed to reach the originator device within a given time span after a message item has been issued by the originator device (i.e. The request message 77 may take a variety of different formats, including the formats and protocols of existing industry standards. Slight variations may be required to use some of the existing protocols. For example, the de facto industry standard for requesting a digital certificate for a public/private key pair is defined by a protocol known as the PKCS#10 protocol. PKCS#10 messages are self-signed to provide proof-of-possession of the corresponding private key. In the case of real -time status checking, the requesting party (i.e., the relying party 62) is not normally the same entity as that possessing the key pair in question, and

thus does not possess the private key. Thus, if PKCS#10 message format is to be used, the certificate authority 66 is altered so as to receive a public key, an existing digital certificate, or both of these items with additional information. For example, the request could be slightly altered so as to distinguish the request from a standard PKCS#10 message by adding header information or the like identifying the request as a real -time status inquiry of an existing digital certificate or public key.) [column 6, lines 32-51]; and

asking the recipient device for a signed statement indicating at least one of a last message item received and a last message item sent by the recipient device [column 6, lines 32-51].

As to claims 31 and 44, Fox discloses the step of storing with at least one of the administrator devices and the administered devices, a history record of communication items exchanged there between, the history record being agreed upon and signed by both the administrator device and the administered device (i.e. FIG. 6 illustrates how accumulated signed receipts, generated as part of the process of selling and re-selling a single transaction, encapsulate the transaction's history. Initially, party A holds transaction T and receipt/certificate Cert.sub.1, which describes how party A came to hold the transaction. Party A proposes to sell the transaction T to party B and sends party B the transaction T along with the receipt/certificate Cert.sub.1 and other supporting evidence, if necessary. Party B evaluates the evidence to see that it satisfies its policy and if so, issues a receipt/certificate ("Cert.sub.2 ") as proof that its policy was satisfied. The new receipt/certificate Cert.sub.2 is returned to party A and the transaction between party A and party B concludes. Party B now holds transaction T, receipt/certificate

Cert.sub.1 (which references T) and receipt/certificate Cert.sub.2 (which references both transaction T and Cert.sub.1).) [column 9, lines 21-36].

As to claims 32 and 45, Fox discloses the step of carrying out at the originator device a session closing step mentioning at least one of a last message item received and a last message item sent by the recipient device (i.e. the relying party's policy is met, step 714 branches to step 718 where the reissue certificate 80 and relying party policy information are combined to form a receipt. The receipt is forwarded to the end entity 60 in step 720) [column 10, lines 43-47].

As to claims 33 and 46, Fox discloses the step of keeping with the originator device an indication of an on-going communication session as a pending session until a signed receipt item is received from the recipient device (i.e. the relying party's policy is met, step 714 branches to step 718 where the reissue certificate 80 and relying party policy information are combined to form a receipt. The receipt is forwarded to the end entity 60 in step 720) [column 10, lines 43-47].

As to claims 34 and 47, Fox discloses the step of inserting in the communication items, payload data and administrative commands accompanied by respective digital signatures (i.e. FIG. 5 shows a financial transaction in which additional local inquiries, other than the status of a public key and/or a digital certificate, may be required by the policy evaluation engine 76. The additional policy information may be requested in the request message 77 and evaluated by the certificate authority 66, or may be determined independent of the certificate authority. If determined by the certificate authority 66, the information is added to the reissue certificate 80. If determined by the relying party, digitally signed signatures 87 or the like regarding the locally determined policy information may be generated and combined with the reissue digital certificate

80 or, alternatively, the relying party may issue another reissue certificate incorporating the new information.) [column 8, lines 54-67].

As to claims 35 and 48, Fox discloses the step of causing the recipient device to verify digital signatures for validity [column 8, lines 54-67].

As to claims 36 and 49, Fox discloses the step of creating digital signatures under the full control of the device issuing such signatures [column 8, lines 54-67].

As to claims 37 and 50, Fox discloses the step of associating secure digital signature evidence with the digitally signed messages and receipt [column 8, lines 54-67]s.

As to claim 42, Fox discloses a system of an administrator device and an administered device in a network, the administrator device and administered device being configured for communication in the form of a chain of digitally signed communication items (i.e. the set of receipts/certificates generated by every transfer of the transaction forms a digitally-signed chain of evidence binding not only every step of the transaction but also every policy application that happened along the way. Of course, it is feasible to include less information than the total accumulated with each additional transaction) [column 9, lines 52-67] including messages sent from an originator device to a recipient device, each the message having associated a respective digitally signed receipt (i.e. the relying party's policy is met, step 714 branches to step 718 where the reissue certificate 80 and relying party policy information are combined to form a receipt. The receipt is forwarded to the end entity 60 in step 720) [column 10, lines 43-47], and wherein the originator device is configured not to send a new item toward the recipient device in the absence of a respective digitally signed receipt for a previously sent item [column 10, lines 48-58].

As to claim 55, Fox discloses a communication network comprising a system [column 4, lines 30-43].

As to claim 56, Fox discloses a computer program product, loadable in the memory of at least one computer, and comprising software code portions capable of performing the steps of the method [column 3 line 65 to column 4 line 16].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 38 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox et al U.S. Patent No. 6,842,863 B1 (hereinafter Fox) as applied to claims 29 and 42 above, and further in view of Fiat U.S. Patent No. 4,964,164.

As to claims 38 and 51, Fox teaches digital signatures [column 8, lines 54-67].

Fox does not teach that the secure digital signature evidence is in the form of RSA class digital signatures.

Fiat teaches the use of RSA digital signatures and the benefit of using such a scheme [column 3, lines 30-62].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Fox so that the digital signatures employed by Fox would have been RSA type signatures.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Fox by the teaching of Fiat because the RSA algorithm provides an elegant means for fulfilling these requirements, by using the RSA algorithm as digital signature exponents. The sender of a signature represented as a signed-message-data signal can sign his signature using his own secret key, which is normally the decryption key. The signing of a signature using one's own secret key can be viewed as taking the eth root of a signature, modulo n. Anyone can verify the signed-message-data signal using the sender's published key, e. The verification of the signature represented as a verified-message-data signal can be viewed as raising the signed-message-data signal to the eth power, modulo n. If this verification produces the correct verified-message-data signal, then the signed-message-data signal can only have come from the appropriate sender, and thus both its contents and origin have been authenticated. Note, however, that the verification no longer offers protection against disclosure of contents, as anyone can verify the signed-message-data signal using the public key exponent [column 2, lines 37-56].

8. Claims 39-41 and 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox et al U.S. Patent No. 6,842,863 B1 (hereinafter Fox) as applied to claims 29 and 42 above, and further in view of Wildish et al US 2003/0115457 A1 (hereinafter Wildish).

As to claims 39-41 and 52-54, Fox the steps of arranging communication between a set of administrator devices (i.e. relying party 62) and a given administered device (i.e. end entity 60).

Fox does not teach permitting at least one administrator device in the set to hide its identity to the administered device. Fox does not teach the step of hiding the identity of the at least one administrator device to the administered device by using at least one of group

signatures or pseudonym digital certificates. Fox does not teach the step of resuming a session interrupted in the absence of a receipt provided by the at least one administrator hiding its identity to a message sent by the given administered device, wherein the session is resumed by the at least one administrator hiding its identity.

Wildish teaches a device hiding its identity by using pseudonym digital certificates [0019-0022].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Fox so that the relying party 62 would have had the ability of hiding its identity to the end entity 60 by the use of pseudonym certificates. A session would have been interrupted in the absence of a receipt provided by the at least one administrator hiding its identity to a message sent by the given administered device. The session would have been resumed by the at least one administrator hiding its identity.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Fox by the teaching of Wildish because the use of compact pseudonyms in public key certificates also provides a low-overhead method to reference a certificate chain that can be used to verify the authenticity of an end-entity's digital certificate. In many standard security protocols such as TLS, WTLS, SSL or S/MIME, an entity using a digital certificate to authenticate itself generally provides a list of digital certificates that can be used to construct a chain for some other party to verify the authenticity of the entity's certificate. For applications over constrained networks such as wireless networks, this increases the bandwidth used. Further, for constrained devices such as smartcards or mobile phones, there may be limited storage space to store the required certificates. An improved method of conveying information

used to construct the certificate chain is needed and this invention is an effective method of identifying the certificate chain as a concatenation of pseudonyms [0011].

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131